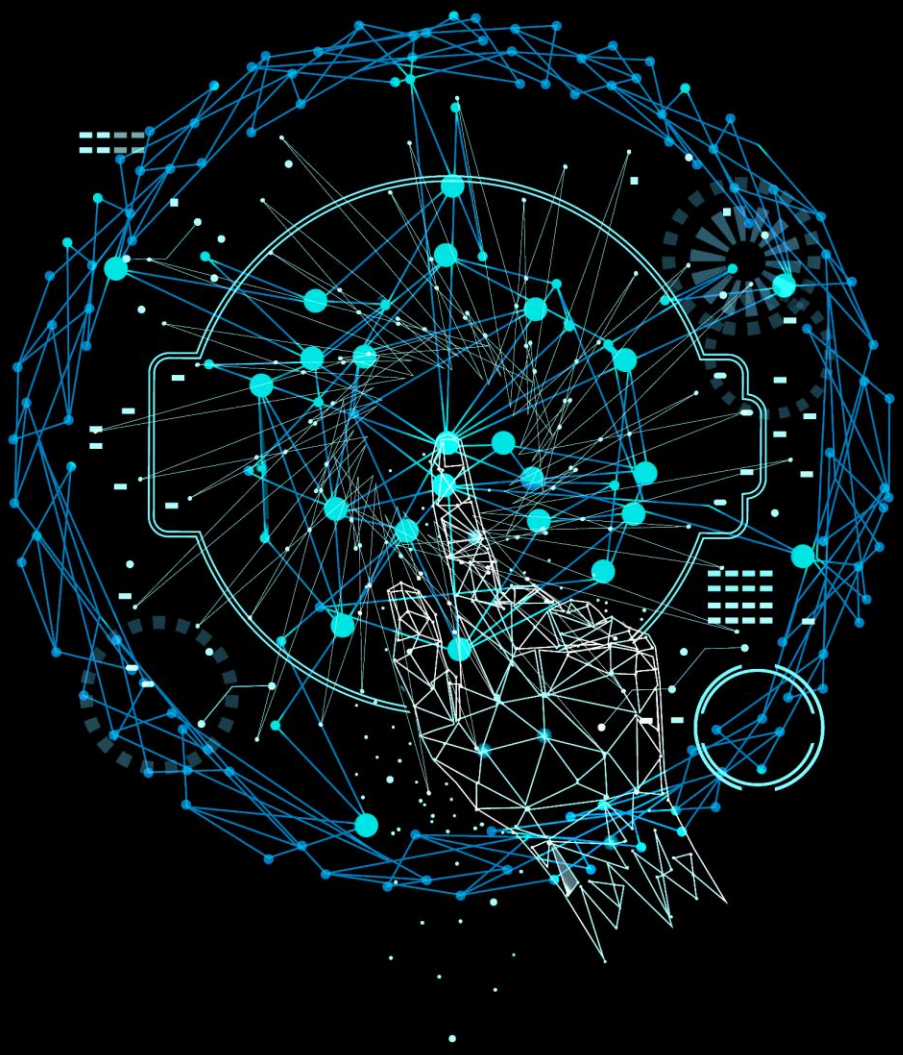
Deloitte.



Mobile Application Security Testing

April 2019

OUR UNDERSTANDING

- Mobile devices have become a part of our life and the applications on them are a dominant form of digital interaction. All of us use at least four to five mobile apps every day. We can check everything on apps – right from our bank account balance and latest scores of different sports to shopping for an outfit to finding directions to a restaurant. There's an app for almost everything.
- Mobile apps play a very prominent role to drive the business of every organisation today. Given the increased usage by organisations, it is crucial to secure these mobile apps to preserve and improve business' reputation.
- It is imperative that user data, company data, and intellectual property is secured and handled properly on all mobile apps. Hence, mobile app security testing is critical to meeting today's security threats. However, a one-size-fits-all approach to mobile app security testing isn't sufficient, because every mobile app is unique and requires a different level of security.
- Our comprehensive mobile security testing approach and methodology have been developed after performing several mobile app security assessments across various clients in different sectors such as banking, finance, healthcare, indoor navigation, technology, and IoT solutions.

Our comprehensive mobile security testing approach will cover all the possible threats and attack vectors that affect the mobile app landscape.

Typical challenges in mobile application security testing

Blind spot while scoping

During scoping and coverage when traditional security testing approach is followed, different areas in the mobile app ecosystem lead to "blind spots".

Standard threats and risks

A one-size-fits-all approach to mobile app security testing isn't sufficient, because every mobile app is unique and requires a different level of security.

Mobile app testing environment

Mobile apps face device compatibility issues and device farm of jailbroken iOS and rooted Android devices along with specialised tools are required to execute fine grained mobile app security tests.

Skill sets

Mobile app security testing requires various skill sets to work together, which is often challenging.

OUR VALUE PROPOSITION

MOBILE PENTESTING SETUP

Device farm made up of JB/rooted/non-JB/non- rooted devices running different OS versions. This ensures mobile app compatibility and execution of high percentage of planned security tests

TEST CASES

50+ security tests formulated for both android and iOS applications

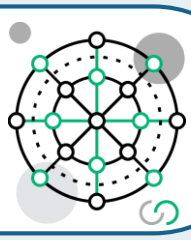
RUNTIME ANALYSIS

Usage of specialised tools and techniques w.r.t. advanced mobile application testing

DEPLOYMENT SOLUTION AND CONFIGURATION

Employ techniques to bypass certificate pinning, rooted/jailbroken device, debug and tamper detections, loopholes in settings and configurations of device management solutions

MOBILE APPLICATION SECURITY TESTING COVERAGE AREAS



APPLICATION LEVEL

(Mobile and server side)

- Server side penetration testing
- Back end services and Application Program Interface (API) testing

Improper session management

Weak server-side controls

MOBILE DEVICE LEVEL

- Reverse engineering and code analysis
- Data storage and forensic analysis

Stealing sensitive information

File analysis

TOOL KIT FOR MOBILE APP SECURITY TESTING

- QARK
- AndroBugs
- MobSF
- Clangs iOS Analyser
- Burp Proxy
- Apktool
- MobSF
- Drozer
- iFunBox
- Appie
- iExplorer
- Frida

SELECT CREDENTIALS

CASE STUDY 1

A leading solution provider in virtualisation and cloud: Mobile application security assessment of 20+ enterprise-level mobile applications

Overview	• Client is a global firm headquartered in the US and has presence in many countries including India. • Client engaged Deloitte to assist it to perform mobile app security assessment of 20+ enterprise-level mobile apps.
Actions	• Performed in-depth mobile app security assessment for mobile apps (Android and iOS) that belong to different categories such as finance, IoT, indoor navigation, business, sales • Developed a custom mobile app penetration testing set-up consisting of a device farm made up of a combination of rooted/non rooted Android devices and jailbroken/non-jailbroken iOS devices • Formulated a comprehensive mobile app security checklist comprising 50+ security tests for both Android and iOS
Outcomes	• 100+ critical flaws identified and immediately remediated by the concerned mobile app teams • Several security flaws identified in device management platforms and third-party frameworks used to develop mobile apps • Mobile app pentesting report for one of the important business apps was considered comprehensive for production roll-out by one of the strategic customers of the client • Several unique mobile app vulnerabilities uncovered by using advanced mobile app pentesting techniques such as runtime hooking and binary modification

CASE STUDY 2

A large multinational product-based company: Security assessment of their flagship Learning Management Solution (LMS) mobile application

Overview	The client engaged Deloitte to: • Perform security assessment of their flagship mobile apps (iOS and Android) powered by 100+ APIs • Provide effective remediation for the identified vulnerabilities and exploits
Actions	• Focused to uncover security vulnerabilities more oriented towards business logic flaws, privilege escalation, and user-role authentication and authorisation • Identified and remediated highly impactful vulnerabilities in mobile apps, which was possible after following a custom mobile pentesting methodology developed by Deloitte
Outcomes	• Most of the reported vulnerabilities (>60%) were classified as zero day in nature and immediate fixes were rolled out considering the criticality and impact • Authorisation-based security flaws helped the client to have a relook at the configured gateway and apply rules consistently across all the incoming service calls • Detailed practical recommendations were provided by Deloitte team to address the critical vulnerabilities in the areas of data storage and forensics

CASE STUDY 3

A large insurance and investment solutions company: Security assessment of their mobile applications

Overview	The client engaged Deloitte to perform mobile app penetration test across their entire application stack consisting of 150+ critical APIs
Actions	• Performed in-depth analysis across mobile app stack to identify the attack vectors, assets, and their value to the business • Identified security vulnerabilities oriented towards business logic flaws, privilege escalation, user-role authentication and authorisation, and password management • False positive analysis of the vulnerabilities reported by automation framework and other scanners • Formal documentation of identified vulnerabilities • Walk-through of vulnerabilities to stakeholders
Outcomes	The programme is still going on, and following are its current outcomes: • Assessed multiple mobile apps powered by 150+ APIs and uncovered a huge number of security loopholes • Helped client to fix the critical, high, and medium rated vulnerabilities in priority to deliver secure applications to its customers • Identified very critical security vulnerabilities in application, which are already in production and helped client to fix them

CONTACT US

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader - Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Santosh Jinugu
Executive Director, Risk Advisory
Deloitte India
sjinugu@deloitte.com

Deloitte.